Rechtliche Aspekte zu Industrie 4.0

Ulrich Herfurth, Rechtsanwalt

MÄRZ 2015

Technologische Entwicklungen entstehen aus realen Bedürfnissen des Marktes und treiben die Entwicklungen in Wirtschaft und Gesellschaft an. Das Recht bildet in der Folge diese neuen Phänomene ab, um Antworten auf dabei entstehende Fragen zu finden und Lösungen für dabei auftretende Konflikte der Beteiligten zu entwickeln.

„Industrie 4.0“ ist zwar ein Schlagwort, markiert aber damit eine technologische und gesellschaftliche Entwicklung von beachtlicher Bedeutung. Zwar erscheinen viele Bausteine im Zusammenwirken der vernetzten Maschinen, Betriebe und Unternehmen als bereits bekannt, tatsächlich wird die Dimension der Datenvernetzung in der Rechtspraxis letztlich dazu führen, dass heutige rechtliche Instrumente faktisch nicht mehr so einsetzbar sind, wie wir sie kennen.

Das Recht ist lebendig und passt sich neuen Gegebenheiten und Anforderungen an, durch privatautonome Vertragsgestaltung, durch Rechtsprechung und durch Gesetzesänderungen – und zwar in der Regel in dieser zeitlichen Reihenfolge. Für die Entwicklung zu Industrie 4.0 ist daher geboten, dass sich die Rechtssetzer und die Rechtsanwender frühzeitig und vorausschauend mit möglichen neuen Entwicklungen auseinandersetzen, um dazu Lösungen vorzubereiten. Systemimmanent ist dabei, dass dies eine Auseinandersetzung auf der Grundlage von zahlreichen

Unbekannten bedeutet und die rechtliche Betrachtung mit Szenarien und Annahmen arbeiten muss.

Erst im letzten Jahr hat eine spürbare rechtliche Auseinandersetzung mit der Thematik begonnen, die nun weiterzuführen und zu vertiefen ist.

Technologische Entwicklungen im rechtlichen Kontext

Schlaglichter

- Rechtswidrige Technologie lässt sich nicht vermarkten
- Der Rechtsrahmen wird zunehmend europäisch und international
- Neue Technologien sind oft nicht genau in vorhandenem Recht abgebildet
- Aber das Recht ist anpassungsfähig über Gesetzgebung und Rechtsprechung
- In Südkoreas Ethikcharta: „Menschen und Roboter müssen die Würde des Lebens, die Informations- und Technikethik respektieren“.
- In Florida, Nevada und Kalifornien gibt es bereits Regelungen für den Einsatz autonomer Fahrzeuge

Die rechtliche Betrachtung der Mechanismen und Abläufe unter Industrie 4.0 zeigt einen breiten Querschnitt von Aspekten. Dieser ist zunächst geprägt durch ein automatisiertes und eigenständig reaktives Zusammenwirken von Ressourcen,
in Konstellationen, die zum Beispiel folgendermaßen kategorisiert werden können:

M2M	machine to machine
P2M	part to machine
M2X	machine to externals
M2S	machine to server
S2PRI	server to printer
S2L	server to logistics
P2L	part to logistics
H2M	human to machine

Aus all diesen Konstellationen leiten sich unterschiedliche rechtliche Fragen ab, die anhand der entsprechenden Prozesse dargestellt werden können. Im Folgenden sind einige der bereits in Diskussion befindlichen sowie weitere Fragen dargestellt.

Rechtliche Themenfelder zu Technologie

Die klassische juristische Sichtweise orientiert sich nach Rechtsgebieten, anhand derer die im Unternehmen auftretenden Problemstellungen erfasst werden können. Dazu wird sich eine Betrachtung von Industrie 4.0 zunächst an die wichtigsten rechtlichen Felder anlehnen, die auch bereits heute im Verhalten von Unternehmen im Betrieb, im Markt und gegenüber Geschäftspartnern eine Rolle spielen:

- Gewährleistung
- Garantiehaftung
- Deliktische Verschuldenshaftung
- Gefährdungshaftung, Produktsicherheit, Produkthaftung
- Strafrechtliche Haftung
- Arbeitsschutz, Betriebssicherheit, Gesundheitschutz
- Umweltschutz
- Wettbewerbsrecht
- Gewerblicher Rechtsschutz
- Datenschutz, Informationelle Selbstbestimmung
- Datensicherheit, Geistiges Eigentum
- Vermögensschutz, Eigentumsschutz

Allerdings stammt diese Strukturierung eher aus einer reaktiven Sichtweise, nämlich der nachträglichen Prüfung von Sachverhalten auf ihre rechtlichen Folgen hin.

Rechtliche Themenfelder nach Unternehmensbereichen

Für die vorausschauende rechtliche Unternehmensberatung ist hingegen eine an Unternehmensprozessen orientierte Betrachtung erforderlich. Diese Prozesse müssen in der juristischen Bewertung abgebildet werden. Da zu Industrie 4.0 die Prozesse, Zusammenhänge und Wirkungen naturgemäß noch nicht vollständig und abschließend erkennbar sind, hilft die Entwicklung von Szenarien, um mögliche Situationen technologisch, ökonomisch und juristisch zu profilieren und dazu Beurteilungen und Maßnahmen zu entwickeln. Die Prozesse lassen sich zunächst den wichtigen Unternehmensbereichen zuordnen:

- Forschung und Entwicklung
- Produktion
- Logistik
- Produkte
- Informationstechnologie und Daten
- Markt und Kunden
- Wettbewerb
- Personal und Arbeit
- Steuern und Finanzen
- Geschäftsführung und Aufsicht

Forschung und Entwicklung

Die Entwicklung neuer Prozesse und Produkte ist eine ständige Herausforderung für Unternehmen. Dabei nimmt ein systematisches Wissensmanagement eine wichtige Rolle ein. Wissen wird von Menschen generiert – im eigenen Betrieb oder bei Forschungs- und Entwicklungskooperationen bei Vertragspartnern. In beiden Konstellationen nehmen die Herausforderungen im Management des Wissens und in der Zuordnung der Ergebnisse deutlich zu. Die mächtigen Aufgaben im Industrie 4.0 – Wissen liegen in der rasch steigenden Komplexität mit vernetzten Partnern und der weitreichenden Spanne fachlicher Kenntnisse über Produktion, Maschinenbau und Informationstechnologie. Die aktuellen Kooperationen von Maschinenbau und Fahrzeugbau mit globalen Daten- und Internetkonzernen machen dies deutlich. Erste Fragen:

- Wer sollte an einer interdisziplinären Zusammenarbeit beteiligt sein?
- Wie lässt sich diese organisieren / arrangieren?
- Wie kann Überwachung nach innen und von außen erfolgen?
- Welche Zertifizierungssysteme sind verfügbar und geeignet?
- Wem stehen die Ergebnisse zu?
- Wer darf die Ergebnisse nutzen?
- Wie werden Mitarbeiter angemessen und rechtssicher an ihren Entwicklungen und Erfindungen beteiligt?

Produktion

Viele Betrachter sehen zurzeit die wesentlichen Änderungen hin zu einer Industrie 4.0-Struktur in der Produktion. Tatsächlich sind es die betrieblichen Abläufe und Prozesse, die durch digitale Vernetzung und automatisierte Vorgänge und Entscheidungen verändert werden; dabei stützen sich die Beteiligten auf ihre Erfahrungen aus CAM und CIM und denken diese in einer weiter intensivierten Verdichtung der Abläufe fort. Ob dies allein ausreicht, muss sich zeigen - die Entwicklung kann durchaus mit der Potenzierung von

Datenmengen und Interaktionen sprunghaft eine neue Dimension erreichen, bei der die bisherigen Instrumentarien zur Steuerung nicht mehr ausreichen.

Unternehmensinterne Produktion

Internes Qualitätsmanagement

Die detaillierte Strukturierung der Produktionsabläufe folgt heute nicht nur technischen oder organisatorischen Normen, sondern Industriestandards und Unternehmens-Policies für Effizienz und Qualität. In Maschinenbau, Automotive und Aviation sind Qualitätsmanagementsysteme feste Grundlage der Produktion. Letztlich richten sich die Anweisungen und Handhabungen darin heute an die Menschen, die in der entsprechenden betrieblichen Aufgabe Verantwortung tragen. Sobald Maschinen und Systeme aber selbst verantwortliche Entscheidungen treffen, muss das Unternehmen neue Strukturen schaffen, die das verantwortliche Zusammenspiel von Mensch und Maschine neu definieren.

- Definition des QM durch das Management
- Automatische Fortschreibung aus Prozessdaten?
- Inhalte des QM-Manuals anpassen?
- Aufbau des QM-Manuals verändern?
- Art und Inhalt der Schulungen verändern?
- Überwachungs- und Kontrollinstrument im QM-Manual ändern?
- Definition von Schnittstellen der Maschinen im Betrieb zur Fehleridentifikation (wg Haftung des Maschinenherstellers)
- Datenmanagement / DM-Vereinbarungen / IT-Compliance (siehe unten "Daten")
- Outsourcing / Cloudmanagement / Vereinbarungen (siehe unten "Daten")

Internationale Arbeitsteilung im Konzern

In internationalen Konzernen, aber auch mittelständischen Unternehmen mit Betrieben im Ausland stellen sich spezifische Fragen zum Grenzübertritt von Leistungen und Produkten im automatisierten Prozess mit neuer Schärfe. Wenn also der Konzern Daten über Ländergrenzen austauscht, ins Ausland sendet oder Personen aus dem Ausland den Zugriff auf Daten im Inland (Europa) erlaubt, stellen sich erneut Fragen:

- Welche nationalen / supranationalen / internationalen Datenschutzvorschriften sind zu beachten (z.B EU / Drittländer)?
- Haben die Daten einen Wert? Gilt die Überlassung als Lizenz? Sind dazu steuerliche Bestimmungen zu Verrechnungspreisen zu beachten?
- Werden Daten im Konzern ausgelagert? Zentralisiert?
- Entsteht dadurch eine steuerliche Betriebsstätte im Ausland?
- Wie wären dann die Erträge der Betriebsstätte zu ermitteln?
- Sind für die Überlassung von Daten im Konzern in das Ausland für Deutschland geltende Exportkontrollvorschriften zu beachten (Außenwirtschaftsgesetz, UN-Embargo, US-Embargo)?
- Sind für die Überlassung von Daten im Konzern in das Ausland dortige Importkontrollvorschriften oder Zollvorschriften zu beachten?
- Sind für die Überlassung von Daten im Konzern aus dem Ausland deutsche Importkontrollvorschriften oder Zollvorschriften zu beachten?

Arbeitsschutz, Betriebssicherheit, Gesundheitsschutz

Die automatisch gesteuerte und selbst entscheidende Maschine wird ein neuer „Arbeitspartner“ der Mitarbeiter. Kommt es sprichwörtlich zur „Arbeit Hand in Hand“, lassen sich die bisherigen Sicherheitskonzepte nicht mehr aufrechterhalten, etwa das Kapseln der Roboter in Käfigen. Berührungsfähige Systeme müssen neue Sicherheits- und Kontrollmechanismen umfassen, die wiederum den Mitarbeiter nicht seiner humanen Arbeitsweise berauben dürfen. Die Systeme müssen so angelegt sein, dass klar ist, wem das sicherere Verhalten zugetraut wird, dem Mitarbeiter oder dem intelligenten System.

- Darf sich das Konzept 4.0 hinsichtlich des Arbeitsschutzes (Lärm, Geruch, Verletztungsgefahr) zu Lasten des einzelnen Arbeiters auswirken?
- Muss / soll / kann mit Rücksicht auf die Gefahrenquelle differenziert werden?
- Sollen Menschen oder Maschinen Aufsicht / Kontrolle über Maschinen ausüben?
- Müssen/dürfen maschinelle Entscheidungen automatisch dokumentiert und aufbewahrt werden?
- Müssen / dürfen menschliche Entscheidungen automatisch dokumentiert und aufbewahrt werden?
- Ist "Outsourcing" möglich, wenn die Schnittstellen / Grenzen zwischen den Unternehmen immer weicher werden.

Umweltschutz

Es versteht sich, dass auch reaktive Systeme so angelegt sein müssen, dass Umweltvorschriften eingehalten und Umweltgefahren vermieden werden. Darüber hinaus bietet Industrie 4.0 die Chance, dass intelligente Systeme umweltfreundlicher agieren, weil sie in der Lage und darauf eingestellt sind, ihr Verhalten zu optimieren. Konzeptionen zum *smart home* und Energie-Managmentsysteme in Betrieben weisen bereits heute die Richtung:

- Darf sich erhöhter Energiebedarf zu Lasten der Natur auswirken?
- Zulässigkeit nur unter Berücksichtigung / Einbeziehung erneuerbarer Energie (Kosteneffizienz)?
- Zulässigkeit nur unter Berücksichtigung / Einbeziehung der "fairen" Rohstoffgewinnung (Konfliktrohstoffe)?
- Wie lassen sich Prozesse energietechnisch optimieren?
- Welche öffentlichen Mittel stehen für Systemverbesserungen, auch durch Software, zur Verfügung?
- Wie gut müssen Maschinen recyclebar sein?

Lieferkette

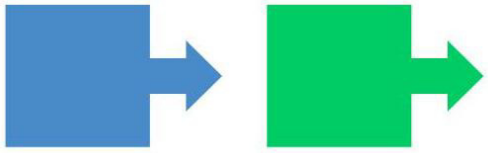
Die bisherige Betrachtung konzentriert sich auf die Prozesse innerhalb eines Betriebes oder zwischen mehreren Betrieben in demselben Unternehmen. Eine neue Herausforderung entsteht, wenn die automatisierten Prozesse unternehmensübergreifend ablaufen. Besondere Bedeutung kommt dabei den zahlreichen Entscheidungsprozessen in den betrieblichen und dann auch geschäftlichen Abläufen zu, die durch intelligente Software auf Grundlage von Algorithmen getroffen werden und nicht mehr durch Willensbildung und Willenserklärungen von Menschen.

Allgemeines

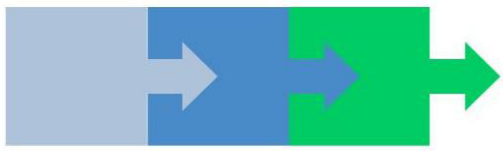
Als Grundlage der geschäftlichen Zusammenarbeit bietet sich zunächst das aus dem Management von industriellen Lieferketten bekannte vertragliche Instrumentarium an, das entsprechend weiterentwickelt werden muss:

- Welche Vereinbarungen müssen in Rahmenlieferverträge neu aufgenommen werden (siehe vor allem unten "Daten")
  - Rahmenvertrag
  - NDA / Vertraulichkeitsvereinbarung
  - QSM Vereinbarung
  - Liefer-AGB
  - Werkzeugüberlassungsvereinbarung
  - Neu: Datennutzungsvereinbarung
- Welches materielle Recht ist in einer internationalen Prozesskette zugrunde zu legen?
- Welche Gerichte sind örtlich zuständig?
- Welche Standorte sind für das anwendbare Recht und den Gerichtsstand maßgeblich (Lieferant, Leistungsempfänger, Prozessrechner, Datenspeicher, juristischer Sitz)
- Welche Auswirkungen hat es, wenn Server im Ausland betrieben werden?

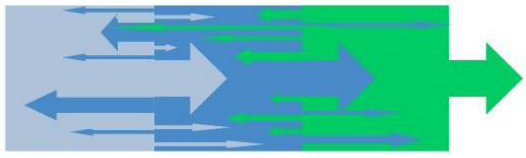
Die Bedeutung der neuen Anforderungen lässt sich erkennen, wenn man sich die Entwicklung der technischen und geschäftlichen Beziehungen der Beteiligten von der Lieferkette bis hin zur integrierten Produktion vor Augen hält:



Lieferbeziehung



Shop in Shop



Industrie 4.0

Industrie 4.0 +

Abb.1:
Schema: Herfurth

Das Bild zeigt schematisch, wie die Abläufe sich ineinander durch Datenströme verflechten und verweben, so dass Leistungsschnittstellen zunehmend schwieriger oder faktisch gar nicht mehr zu identifizieren sind. Allein der organisatorische und wirtschaftliche Aufwand zur Sachverhaltsermittlung und Beweisführung könnte in der Rechtspraxis die Verfolgung oder Verteidigung von Rechten der beteiligten Unternehmen unmöglich machen. Die Dimension von auszuwertenden Daten kann durchaus ungleiche Kräfteverhältnisse weiter vertiefen.

Internationale Arbeitsteilung mit Lieferanten

Im Grundsatz stellen sich bei Auslandbezug mit Geschäftspartnern unter Industrie 4.0 zunächst die gleichen Fragen wie innerhalb eines Konzerns. Hinzu kommen aber die Aspekte, die sich mit Blick auf mögliche rechtliche Auseinandersetzungen ergeben.

Wenn Daten mit Lieferanten oder Kunden über Ländergrenzen ausgetauscht werden / Sendung ins Ausland / Zugriff aus den Ausland:

- Welche nationalen / supranationalen / internationalen Datenschutzvorschriften sind zu beachten (z.B EU / Drittländer)?
- Haben die Daten einen Wert? Gilt die Überlassung als Lizenz? Sind dazu steuerliche Bestimmungen zu Verrechnungspreisen zu beachten?
- Werden Daten im Konzern ausgelagert? Zentralisiert?
- Entsteht dadurch eine steuerliche Betriebsstätte im Ausland?
- Wie wären dann die Erträge der Betriebsstätte zu ermitteln?
- Sind für die Überlassung von Daten an Kunden Antiterrorismusvorschriften zu beachten?
- Liegen Tatbestände für Prüfungen nach dem Geldwäschegesetz vor?
- Sind für die Überlassung von Daten in das Ausland für Deutschland geltende Exportkontrollvorschriften zu beachten (Außenwirtschaftsgesetz, UN-Embargo, US-Embargo)?
- Sind für die Überlassung von Daten in das Ausland dortige Importkontrollvorschriften oder Zollvorschriften zu beachten?
- Sind für die Überlassung von Daten aus dem Ausland deutsche Importkontrollvorschriften oder Zollvorschriften zu beachten?
- Welche Dokumentationspflichten sind zu beachten und wie können diese bei Big Data erfüllt werden?

Gewährleistung der Lieferanten

Eine besondere Bedeutung im Zusammenspiel von Partnern in der Lieferkette erhält aber die Qualität der Produkte unter dem Gesichtspunkt der Haftung für fehlerhafte Leistungen und Mängel. Die informationsgestützte und automatisierte maschinelle Abwicklung von Geschäftsprozessen ersetzt dabei die individuelle Willenserklärung von Menschen. Maschinen haben keinen eigenen Willen; sie sind keine Personen, die Erklärungen abgeben können, sondern sie sind Sachen im Rechtssinne. Die von ihnen gesendeten Befehle und Informationen sind also letztlich den Menschen und damit Unternehmen als Willenerklärung zuzurechnen, die das weitreichend programmierte System so zum Einsatz bringen. Das Recht ordnet solche Systeme daher auch nicht als Vertreter oder Erklärungsboten ein, sondern als so genannte Erklärungsagenten.

- Wer definiert das Produkt bzw. den Vertragsgegenstand?
- Wer trägt Verantwortung für fehlerhafte Übermittlung?
- Welche rechtliche Bedeutung hat die Überlassung von Daten an Produktionspartner (vertraglich vereinbarte Beschaffenheit?)
- Sind automatisierte Prozessbefehle Willenserklärungen?
- Besteht die Pflicht zu einer Warenprüfung? Wenn ja, zu welchem Zeitpunkt (auch Teil- oder nur Endprodukte)?
- Wie weit kann der Datenempfänger mit allgemeinen Geschäftsbedingungen die kaufmännische Untersuchungs- und Rügeobliegenheit ausschließen?
- Welchen Service müssen Hersteller für Instandhaltung und Aktualisierung anbieten?
- Welche Entwicklungsstufen sind als Maßstab maßgeblich?
- Ob und inwieweit sind Haftungsbeschränkungen möglich?
- Wer haftet hier genau?
- Sind Verantwortungssphären (räumlich / zeitlich) überhaupt denkbar?
- Wem sind Fehler in automatisierten Abläufen von Maschinen- und Datenvorgängen zuzurechnen?

- Wer übernimmt Haftung für Menschen und Maschinen, selbst wenn Menschen alles richtig getan haben?
- Müssen/ sollen / können Unterschiede in der Haftung davon abhängig gemacht werden, ob Menschen gehandelt haben?
- Wann (ab welchem Beitrag) kann noch von einer menschlichen Handlung ausgegangen werden?

Logistik

In der Logistik bestimmt die Digitalisierung bereits weitgehend die innerbetrieblichen und externen Abläufe. Wege und Standorte von Material, Teilen, Paketen, Paletten und Containern lassen sich in Echtzeit exakt bestimmen und nachvollziehen. Die Effizienzgewinne, wie etwa bei der Chaotischen Lagerung, sind beachtlich. Die Logistikbranche sieht eine Reihe von Faktoren als Treiber der Entwicklung, so etwa

- intelligente Transportmittel
- M2M-Kommunikation
- Sensorik und Echtzeit-Monitoring
- Predictive Maintenance
- automatisierte Vertragsschlüsse
- elektronische Frachtdokumente
- Cloudplattformen zur elektronischen Steuerung und als Marktplätze
- Einsatz mobiler Endgeräte / BYODs
- private Lieferdrohnen.

Produkte

<u>Gewährleistung gegenüber Kunden</u>

Im Grundsatz stellen sich die Fragen zu Lieferanten spiegelbildlich in der Beziehung zu Kunden.

<u>Garantiehaftung gegenüber Nutzern</u>

Und sicherlich stellen sich Fragen zur Haftung gegenüber Dritten, also Nutzern, die nicht Vertragspartner des Unternehmens sind, mit neuer Intensität, wenn womöglich Teile der Produktionsprozesse außerhalb der Kontrolle des Herstellers liegen:

- Ist eine Garantiehaftung überhaupt noch individuell möglich?
- Inwieweit wird innerhalb der Lieferkette „mitgehaftet“?

<u>Deliktische Verschuldenshaftung gegenüber Dritten</u>

Da sich eine deliktische Haftung auf menschliches Fehlverhalten aufgrund einer menschlichen Willensbildung stützt, stellt sich bei automatisierten Systemen, die Frage nach der zivilrechtlichen und strafrechtlichen Verantwortlichkeit.

- Wer hat im Einzelfall die Herrschaft über die Gefahrenquelle?
- Dürfen / Müssen Algorithmen Leben gegen Leben (rational) abwägen?
- Besteht ein Recht auf irrationale Entscheidungen?
- Welche ethischen Konflikte können entstehen, wenn ein Roboter nicht mehr zwischen Mensch und Maschine unterscheiden kann?

<u>Gefährdungshaftung, Produktsicherheit, Produkthaftung</u>

Die gleiche Frage betrifft die Gefährdungshaftung, die ohne Verschulden einer Person allein aus dem Versagen eines Produkts oder einer Anlage entsteht.

- Ob und inwieweit sind Haftungsbeschränkungen möglich?
- Wer haftet hier genau?
- Sind Verantwortungssphären (räumlich / zeitlich) überhaupt denkbar?
- Wem sind Fehler in automatisierten Abläufen von Maschinen- und Datenvorgängen zuzurechnen?
- Wer übernimmt Haftung für Menschen und Maschinen, selbst wenn Menschen alles richtig getan haben?
- Müssen / sollen / können Unterschiede in der Haftung davon abhängig gemacht werden, ob Menschen gehandelt haben?
- Wann (ab welchem Beitrag) kann noch von einer menschlichen Handlung ausgegangen werden?
- Bedarf es einer menschlichen Kontrolle (und Interventionsmöglichkeit) automatisierter Vorgänge?
- Ist ein Unternehmen, das fremdbestimmt produziert, Hersteller i.S.d. ProdHaftG?
- Wer ist bei 3D-Digitaldruck Hersteller i.S.d. ProdHaftG?
- Kann ein unvorhersehbar agierendes System versichert werden?
- Besteht für jeden Lieferanten in der Kette eine Versicherungspflicht? Sind Einschränkungen

möglich (wenn z.B. einzelne Teilprodukte zum Endprodukt unterschiedliche Beiträge leisten)?

Informationstechnologie und Daten

Die Fragen zur Informationstechnologie sind naturgemäß das Herzstück von Industrie 4.0. Denn die IT-Systeme schaffen und erhalten die Funktionalität der vernetzten Produktion, und die Daten sind der digitale Rohstoff, mit dem die Systeme versorgt werden müssen.

Datensicherheit

Zunächst gilt es, die Daten gegen technische Störungen, Beschädigungen und Ausfälle zu sichern.

Dies ist vorrangig eine technisch-organisatorische Aufgabe, aber auch eine rechtliche Verantwortlichkeit des Managements. Es gehört zu den essentiellen Sorgfaltspflichten der Geschäftsleitung und der Aufsichtsgremien im Unternehmen, die betriebliche Sicherheit so einzurichten, dass Beschädigungen von Vermögensgegenständen, also auch Datenbeständen, verhindert werden.

Bei Unternehmen mit kritischer IT-Infrastruktur ist die Geschäftsleitung aber nicht nur gegenüber dem eigenen Unternehmen verpflichtet, sondern neuerdings auch gegenüber der Allgemeinheit: das neue IT-Sicherheitsgesetz (Gesetz zur Erhöhung der Sicherheit Informationstechnischer Systeme vom 24.07.2015) erlegt betroffenen Unternehmen im Störfall bestimmte Meldepflichten auf. Dadurch soll vermieden werden, dass Angriffe und Störungen auf weitere Systeme übergreifen und dass darauf gerichtete Angriffe abgewehrt werden können. Zu kritischen Infrastrukturen zählen solche in den Branchen Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen - allerdings nur, wenn sie „von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden“. Der Gesetzgeber konkretisiert diese Merkmale derzeit noch genauer. Produktionsunternehmen unterliegen dem Katalog daher als solche nicht. Auch kleine Unternehmen (KMU) dürften kaum betroffen sein. Sie müssen aber jeweils damit rechnen, als Zulieferer und Dienstleister für Unternehmen mit kritischer Infrastruktur in vertragliche Pflichten und Haftung genommen zu werden.

Allerdings verlangt das Gesetz von den Unternehmen mit kritischer Infrastruktur auch, dass sie geeignete Maßnahmen treffen, um Störungen zu vermeiden. Die Störungen können sich dabei auf Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der IT-Systeme, Komponenten und Prozesse beziehen, die für die Funktionsfähigkeit maßgeblich sind. Die erforderlichen Maßnahmen umfassen Infrastruktur, Personal, Störfallmanagement und Abschottungen von Prozessen und Bereichen.

Diese Anforderungen sind zwar öffentlich-rechtlicher Natur, und Verletzungen sind als Ordnungswidrigkeit teilweise mit Bußgeld bedroht, aber daraus lassen sich auch zivilrechtliche Schadenersatzansprüche ableiten. Dabei ist leicht vorstellbar, dass dieser Anforderungskatalog mit der Zeit und in abgestufter Form einen Leitbildcharakter entwickelt, der auch auf an sich nicht vom IT-Sicherheitsgesetz erfasste Unternehmen abstrahlt. Die Pflichten von Vorstand und Geschäftsführung würden dadurch im Rahmen der Business-Judgement Rule stärker konkretisiert.

Datendienstleister

Sobald ein Unternehmen zur Unterstützung oder Sicherung des IT-Betriebs externe Berater, Systemhäuser, Softwareanbieter, Rechenzentren und ganze Outsourcing-Systeme als Dienstleister einsetzt, sind deren Rechte und Pflichten sehr sorgfältig zu vereinbaren: Leistungsumfang, Leistungserfolg, Services, Service-Level, Haftung, faktische Haftungswerte, Versicherungen und anderes. Fragen zur Sicherung sind:

- Wo sollen / dürfen eigene Daten gespeichert werden?
- Wer kontrolliert den Datenaustausch?
- Wie können Daten - insbesondere in einer "Cloud" - gegen Zugriffe Dritter geschützt werden?

Besonders gefährlich können aber Eingriffe von Menschen oder von Menschen gesteuerter Systeme sein. Daher muss das Unternehmen Schutzmassnahmen gegen gleichartige Angriffe treffen, deren Angriffsrichtung und Angriffsmethode unterschiedlich sind und denen daher mit differenzierten Abwehrmaßnahmen begegnet werden muss. Dazu zählen vorrangig:

Schutz gegen externe Datenangriffe durch Dritte

Cyber Crime / staatliche Industriespionage durch ausländische Dienste oder private Spionage durch Wettbewerber. Hier sind vor allem technische und organisatorische Maßnahmen zum Schutz der Daten im Betrieb, in der Auslagerung und beim Transfer zu treffen gegen

- Datenmissbrauch
- Datendiebstahl
- Datensabotage (Blockade, Veränderung)
- Erpressung

Schutz gegen externe Datenangriffe durch Vertragspartner

Dabei gilt zunächst der gleiche Grundsatz wie gegenüber Dritten. Allerdings kommt hier gefahrerhöhend hinzu, dass Geschäftspartner systembedingt gerade Zugriff auf die IT-Systeme und Daten über Schnittstellen und nach Transfers haben müssen. Zu den technischen Sicherungen kommen damit rechtliche Instrumente hinzu, insbesondere vertragliche Verwendungsbestimmungen. Auch hier gelten die Risiken

- Datenmissbrauch
- Datendiebstahl
- Datensabotage (Blockade, Veränderung)
- Erpressung

Wie also können Daten gegen zweckwidrige Verwendung (auch des Vertragspartners) geschützt werden?

Schutz gegen interne Datenangriffe

Eigene Mitarbeiter stellen mit ca. 75% der Fälle von Wirtschaftskriminalität die größte Tätergruppe im Unternehmen dar. Dabei sind es typischerweise vertrauenswürdige und qualifizierte Personen in Schlüsselfunktionen im Unternehmen, die aus diversen Motiven ihre Stellung missbrauchen zu

- Datenmissbrauch
- Datendiebstahl
- Datensabotage (Blockade, Veränderung)
- Erpressung

Sicherlich werden Unternehmen mit Mitarbeitern vertragliche Regelungen zum Schutz des Unternehmens treffen, aber auch technologische Kontrollsysteme installieren müssen, die gerade dann eingreifen, wenn sich ein Mitarbeiter bewusst vertrags- und rechtswidrig verhält.

- Wer hat für eine fehlerfreie Übermittlung zu sorgen?
- Wer gilt als Verursacher, wenn die Grenzen nicht erkennbar sind?

<u>Computerstrafrecht</u>

Der Bedeutung von Daten als Wirtschaftsgut hat der Gesetzgeber mit den Straftatbeständen der Datenveränderung in § 303a StGB und der Computersabotage in § 303b StGB Rechnung getragen. Diese Normen ahnden das Löschen, Unterdrücken, Unbrauchbarmachen und Verändern von fremden Daten durch Unbefugte sowie erhebliche Störungen von Datenverarbeitungsanlagen durch Zerstörung, Beschädigung, Unbrauchbarmachung, Beseitigung oder Veränderung von Anlagen oder Datenträgern. Die Taten können im besonders schweren Fall mit bis zu zehn Jahren Freiheitsstrafe belegt werden, insbesondere wenn dadurch ein Vermögensverlust großen Ausmaßes herbeigeführt wurde. Das dürfte bei einem Cyberangriff auf ein Unternehmen in der Produktionskette regelmäßig der Fall sein.

Zwar liegt die strafrechtliche Verfolgung primär im Interesse des Staates und nicht unmittelbar im Interesse des geschädigten Unternehmens – aber oft kann erst die Beteiligung am Strafverfahren als Anzeigeerstatter oder Nebenkläger dem Geschädigten Erkenntnisse zur Tat verschaffen, die nur im Rahmen eines strafrechtlichen Ermittlungsverfahrens gewonnen werden können. Ein Verantwortlicher im Unternehmen wird kaum auf diese Quelle als Grundlage für einen etwaigen zivilrechtlichen Haftungsprozess verzichten können. Dies gilt auch und gerade für Ermittlungen bei mutmaßlichen Angriffen aus den Reihen der eigenen Belegschaft.

<u>Versicherung von Cyberrisiken</u>

Versicherer erwarten, dass Cyberrisiken wachsende Bedeutung erlangen und dass der Bedarf an Versicherungen gegen Cyberrisiken wächst. Die bisherigen Modelle der IT-(Hardware) Versicherung, Software-Versicherung, Betriebshaftpflichtversicherung und der Vertrauensschadenshaftpflichtversicherung decken Cyberrisiken nicht oder nur teilweise ab. Erste Policenmodelle zum Schutz gegen Cyberrisiken sind auf

dem Markt und umfassen zusätzlich auch Assistenz im Schadenfall.

Datenschutz, Informationelle Selbstbestimmung

Aus Sicht der Mitarbeiter und der Kunden kommt dem Datenschutz unter Industrie 4.0 erhöhte Bedeutung zu. Die Zuordnung von Daten als technische oder aber personenbezogene Daten ist oft umstritten, weil letztere dem gesetzlichen Personendatenschutz unterfallen. Damit ist deren Umgang streng reglementiert und auch Gegenstand von arbeitsrechtlichen individuellen oder kollektiven Regelungen und Vereinbarungen. Einige Frage dazu sind:

- Müssen Bereiche existieren, in denen eine Datenerhebung untersagt ist?
- Welche Prozessdaten sind personenbezogene Daten (Kameraüberwachung von Arbeitsprozessen aus Sicherheitsgründen / Kooperation Mensch / Roboter)?
- Wie ist die Sammlung sensibler Daten Dritter zu beurteilen?
- Dürfen/müssen (relevante) Daten an (Sicherheits-)Behörden weitergegeben werden?
- Inwieweit dürfen Datenschutzbestimmungen (angesichts der Rechte Dritter) für Parteien disponibel sein?
- Wie muss die IT-Compliance-Struktur im Unternehmen geändert werden?
- Welches Datenschutzrecht gilt bei Auslandsberührung, also Datentransfer, Datenzugriff, Datenbearbeitung?

Vermögensschutz, Eigentumsschutz

Letztlich befürchten viele Unternehmen, dass sie die Hoheit über ihre Daten verlieren, weil sie bei anderen zumindest in Kopie lagern, im Rahmen der Produktion verändert werden, mit anderen Daten vermischt, aggregiert und ausgewertet werden und damit letztlich neue Datenbestände geschaffen werden. Fraglich ist also, wem an welchen Beständen primäre und sekundäre Rechte zustehen und wie diese gesichert und durchgesetzt werden können.

Ob die bisherigen Instrumente wie Urheberrecht und Schutz von Datenbanken ausreihen, um das neue Spektrum abzudecken, ist noch Gegenstand der Diskussion. Interessant wäre es, Rechtsinstrumente aus dem Sachenrecht für physische Gegenstände auf Daten zu übertragen.

Fragen sind dann:

- Übertragung von Rechtsfiguren des Sachenrechts auf IP (Dateneigentümer, Datenbesitzer, Datenverwahrung, Datennutzungsrechte, Datenmiete, aber auch Datenlizenz)
- Wem gehören die Daten? Wer ist Dateneigentümer?
- Wer ist Datenbesitzer?
- Muss (ggf.: wie kann) verhindert werden, dass Daten über den konkreten Anlass hinaus genutzt werden?
- Begründet die über den konkreten Anlass hinaus getätigte Nutzung Ansprüche für den Datenlieferanten?
- Wer hat das Recht an Sekundärdaten, die sich aus Primärdaten ergeben?
- Darf der Datenempfänger überlassene Daten (anonym) auswerten?
- Darf der Datenempfänger überlassene Daten (anonym) von mehreren Überlassern auswerten / aggregieren / analysieren?
- Muss der Datenempfänger Informationen / Analysen / Auswertungsergebnisse an die Lieferanten der Primärdaten zurückgewähren / Einblick einräumen?
- Wie müssen / können solche Datenrechte und -pflichten in einer hoch verdichteten Datenmischbasis in einer Lieferkette / Prozesskette zugeordnet werden?
- Wie ist der Wert des Eigentums an einer Sache zu beurteilen, wenn diese ohne geeignete Software und Datenzufluss ihre Funktion nicht erfüllen kann?

Provider und Plattformen

In der vernetzten Produktion wird es einen erheblichen Bedarf an Infrastruktur für das Vorhalten, den Austausch und die Verarbeitung von Daten geben. Dabei sind Strukturen nach ihrem Zweck zu unterscheiden, ob sie lediglich unilateral durch ein Unternehmen genutzt werden oder multilateral durch mehrere bzw. viele Teilnehmer.

Provider

Unilaterale Strukturen dienen den Interessen eines Unternehmens, indem dieses seine Daten und Prozesse an ein konkretes Rechenzentrum (*Host*) oder an Anbieter von Serverkapazitäten (*Cloud*) auslagert, gegebenenfalls auch mit ausgelagerter Software (*Software as a service*) oder als ausgelagerte

Gesamtabwicklung von betrieblichen Funktionen (*Outsourcing*). Dabei können diese Dienste durchaus auch Dritten zur Verfügung gestellt werden, etwa als Online-Bestellplattform, Internetpräsenz, Serviceportal oder anderes – es bleibt aber stets bei dem Angebot des einen Unternehmens.

Die wesentliche rechtliche Problematik besteht dabei in der Gewährleistung der Funktionalität der Providerdienste zur Verfügbarkeit und Sicherheit der Daten, definiert nach Leistungsebenen auf Grundlage vertraglicher Vereinbarungen und Leistungsbeschreibungen (*service level agreements*). Bereits heute dürfte die Leistungsfähigkeit und Sicherheit von Rechenzentren den IT-Strukturen in den meisten Unternehmen überlegen sein, bzw. nicht mit vertretbarem Aufwand von mittelständischen Unternehmen erreichbar sein. Unternehmen, die ihre Daten und Prozesse einem Provider anvertrauen, müssen allerdings nicht nur die Funktionalität vertraglich sicherstellen, sondern auch den Schutz ihrer Daten vor unbefugten Zugriffen. Provider haben regelmäßig kein eigenes begründetes Interesse an den fremden Daten ihrer Kunden, da sie lediglich im Wege der Auftragsverarbeitung damit befasst sind und die Daten nicht integraler Teil einer Produktions- oder Leistungskette sind. Daher dürfen Provider ihre Kundendaten nicht für eigene Zwecke nutzen oder Dritten verfügbar machen. Unternehmen als Kunden sollten sich vom Provider garantieren lassen, dass nur befugte Mitarbeiter Datenzugang erhalten und dass diese durch entsprechende Vertraulichkeitsvereinbarungen verpflichtet werden. Aus Sicht des Unternehmens müssen Unternehmensdaten gegen Einblick Dritter geschützt werden und Personendaten nach den Vorgaben des Datenschutzrechts. Die Bedeutung von Zertifizierungen für Provider wird weiter zunehmen, insbesondere soweit sie die Einhaltung der Vertraulichkeitspflichten des Providers nachweisen.

Auch im Verhältnis zum Provider unterliegt das Unternehmen den nationalen und europäischen Datenschutzbestimmungen, deren Wirksamkeit mit der demnächst zu erwartenden Verabschiedung der Europäischen Datenschutzgrundverordnung deutlich erhöht werden dürfte. Die Auslagerung von europäischem Datenschutz unterliegenden Personendaten auf Server in Drittstaaten ist bislang kaum rechtlich einwandfrei möglich, ebensowenig der Zugriff von dort. Erst jüngst hat der EuGH die von der Europäischen Kommission abgesegnete Praxis zur Datenübermittlung an Empfänger in den USA als unzulässig beurteilt: die staatlichen Zugriffsrechte in den USA lassen sich zwischen Unternehmen nicht wirksam durch Musterklauseln im Sinne eines geschützten Datenumfelds (*safe harbor*) einschränken.

Plattformen

Plattformen dienen als mulitlaterale Strukturen der Verknüpfung vieler, voneinander unabhängiger Nutzer. Sie stellen eine Infrastruktur zur Verfügung, auf der die Nutzer sich bewegen und ohne Zutun des Plattformbetreibers miteinander in Verbindung treten und Transaktionen abwickeln können.

Im Grundsatz sind Plattformen nach ihrer Funktion zu unterscheiden; sie sind Informationsplattform (*google*), Kontaktplattform (*facebook,* diverse Partnersuchportale), Kommunikationsplattform (*whats app*), Archivplattform (*Instagram),* Handelsplattform *(ebay,* Reiseportale*,* Autoportale, Immobilienportale, Finanzdienstleistungsportale*),* Verkaufsplattform *(Amazon),* Zahlungsverkehrsplattform *(paypal)* und anderes mehr. Dabei mischen sich Funktionalitäten im Rahmen von *Social Media* Angeboten, bis hin zu sich widersprechenden Angeboten wie unabhängige Preisvergleiche und Produktverkauf. Ob ein Portal rechtlich eine Plattform darstellt, bestimmt sich nach seiner konkreten Struktur.

Die besonderen rechtlichen Fragen zu Plattformen hängen mit einer nicht immer klar definierten Haftung für die Angebote und Transaktionen ihrer Nutzer zusammen. Grundsätzlich wird ein Plattformbetreiber die Gewährleistung und Haftung für Leistungsmängel seiner Nutzer vertraglich ausschließen, er will nicht für die Qualität der auf der Plattform vertriebenen Produkte rechtlich einstehen müssen, auch nicht für die Seriosität und Bonität von Anbieter und Nachfrager. Dass ein Plattformbetreiber ein geschäftliches Interesse an einem möglichst zuverlässigen Kundenportfolio hat, ist eine andere Frage, die er gerne mittels Kundenbewertungen beantwortet. Ob sich ein Plattformbetreiber auch dann von einer Haftung freizeichnen kann, wenn er die Verkaufsbedingungen für Transaktionen seiner Nutzer einheitlich vorgibt, ist zweifelhaft – er rückt damit möglicherweise aus Sicht des Nutzers nahe an das Bild als Anbieter der Leistung.

Kritisch ist auch die Haftung des Plattformbetreibers für rechtswidrige Inhalte, die von Nutzern eingestellt werden. Während in Kommunikationsplattformen die Verletzung von Persönlichkeitsrechten (eigenes Bild) und öffentlich-rechtlichen Schranken (Gewaltverherrlichung, Volksverhetzung u.a.) im Vorder-

grund steht, liegen die Risiken in Informations- und Handelsplattformen in Verletzungen des Urheberrechts, Designrechts, Markenrechts und anderer gewerblicher oder geistiger Schutzrechte. Die Haftung für derartige rechtswidrige Inhalte wird zurzeit von der Rechtsprechung nicht einheitlich behandelt: regelmäßig ist ein Plattformbetreiber verpflichtet, auf Verlangen des Verletzten rechtswidrige Angebote auf seiner Plattform zu entfernen, stets wenn eine gerichtliche Verfügung dies anordnet. Die Rechtsprechung hat aber inzwischen in Einzelfällen auch die Forderung aufgestellt, dass der Plattformbetreiber verpflichtet sein soll, die Rechtmäßigkeit der bei ihm eingestellten Angebote eigenständig zu überprüfen, jedenfalls wenn es sich um Wiederholungen einer bereits festgestellten Verletzung handelt. Gegen derartige Prüfungspflichten wenden sich die Plattformbetreiber mit dem Argument, dass eine Plattform einer Messe, einer Börse oder dem Anzeigenteil einer Publikation vergleichbar sei, nicht aber selbst Anbieter ist. Die Unterscheidung ist deshalb von Brisanz, weil die Entfernung von Inhalten nur eine Unterlassungspflicht darstellt, eine Verletzung einer Prüfungspflicht aber einen Schadensersatzanspruch mit weitreichenden Folgen begründen könnte.

Die bislang überwiegend in Sozialen Medien und in Handelsplattformen auftretenden Verletzungen können in ähnlicher Form auch in industriellen Plattformen auftreten, etwa für den Einkauf, in der Logistik oder zum Personaleinsatz (*crowd working*). Dabei kann es sich um Verletzungen von technischen Schutzrechten (Patente, Muster, Design, auch Urheberrecht für Software) handeln, aber auch um die Bereitstellung von rechtswidrig erlangten Personendaten oder Unternehmensdaten. Greift ein Verletzter oder vermeintlich Verletzter die Veröffentlichung einer Information auf der Plattform an, kann die Entscheidung zur Entfernung des Angebots erhebliche wirtschaftliche Folgen für den Plattformbetreiber und den Anbieter mit sich bringen. Der Plattformbetreiber wird wegen des Schadenersatzrisikos dazu neigen, dem Verlangen nach dem Entfernen des Angebots nachzukommen, der Anbieter verliert damit zumindest vorübergehend sein Angebot auf der Plattform und damit möglicherweise Geschäft.

Telekommunikation

Die Übermittlung von Daten und das Angebot von Diensten im Rahmen der M2M-Kommunikation können die Beteiligten bestimmten Pflichten aus dem Telekommunikationsrecht unterwerfen.

Die Übermittlung von Daten stellt rechtlich in der Regel Telekommunikation dar und umfasst häufig Telekommunikationsdienste im Sinne des Telekommunikationsgesetzes (TKG). Es kommt dabei nicht darauf an, dass die Informationen in der Telekommunikation von Mensch zu Mensch übermittelt werden.
Die Kommunikationsinfrastruktur besteht zumeist in Form von Mobilfunknetzen, so dass die Netzbetreiber „Erbringer“ der TK-Leistungen sind, Vertragspartner für bestimmte Dienste „Teilnehmer“ und die Kunden der Dienste, z.B. Fahrer von *Connected Cars*, „Nutzer“ im Sinne des TKG.

Ob es sich bei M2M-Kommunikationsplattformen um Telekommunikationsdienste handelt, hängt von der konkreten Funktion ab: die Übermittlung von Steuersignalen von und an beteiligte M2M-Geräte ist in der Regel ein Telekommunikationsdienst, bei der Bereitstellung von Inhalten auf der Plattform zum Abruf durch Nutzer ist die Übermittlung hingegen nicht das wesentliche Element. Zur Abgrenzung des Charakters gemischter Dienste wird gerne das ISO/OSI Schichtenmodell für Internetdienste herangezogen. Die Schichten 1 bis 4 haben eher Übertragungscharakter, die Schichten 5 bis 7 eher Inhaltscharakter.

M2M-Dienste stellen in der Regel nicht die Übertragung von Informationen in den Vordergrund, sondern Inhalte und Funktionalitäten wie z.B. Fahrzeugdaten (Fahrweise, Ortung); sie sind damit typischerweise keine Telekommunikationsdienste, sondern Telemediendienste im Sinne des Telemediengesetzes (TMD).
Unterfällt ein M2M-Dienst dem TKG, hat der Erbringer der Dienste eine Anzahl von Pflichten zu erfüllen, die sich auf Kundenschutz, Frequenznutzung, Nummerierung, Fernmeldegeheimnis und TK-Überwachung beziehen.

Markt und Kunden

Bei dem Begriff Industrie 4.0 steht zunächst die Vorstellung betrieblicher Abläufe im Vordergrund. Tatsächlich beginnt aber die Informationskette bereits ganz am Anfang, also beim Kunden, der produktionsrelevante Daten generiert und damit künftig unmittelbar Prozesse auslöst. Die Informationen drin-

gen dabei durch mehrere Stationen der Liefer- und Wertschöpfungskette. Bekannt ist dieser Vorgang bereits bei der Konfiguration von Autos durch die Kunden, die künftig im Online-Modus unmittelbar Produktionsdaten an den Autohersteller (OEM) und durch ihn an dessen Zulieferer von Tier 1 bis Tier 4 übermitteln.
Dabei sind die Daten nicht nur für die konkrete technische Herstellung relevant, sondern auch und mit wachsender Bedeutung als Kundendaten zur Bewerbung und dem Ausbau weiterer Geschäftsbeziehungen. Wenn die Daten nicht nur technische Funktion haben, sondern die persönlichen Vorstellungen und Werte des Kunden widerspiegeln, handelt es sich um Personendaten, die dem Datenschutz unterliegen. Auch hier steht die Frage im Raum, welcher Empfänger die Daten nutzen darf und in welchem Umfang. Wichtige Fragen sind:

- Welche Daten werden von Kunden generiert und unmittelbar in den Produktionsprozess eingespielt?
- Wie darf das Unternehmen diese Kundendaten individuell oder kollektiv nutzen?
- Inwiefern und in welchem Umfang darf ein Unternehmen Daten seiner Kunden an seine Geschäftspartner weitergeben?
- Welche Pflichten muss das Unternehmen seinen Geschäftspartnern auferlegen und überwachen?

Wettbewerb

Die enge Vernetzung von Datenbeständen und Informationen führt zwangsläufig zu einer Verdichtung der Beziehungen der Beteiligten untereinander. Geschäftspartner wissen mehr voneinander als Dritte und können dieses Wissen in neuer Dimension einsetzen, um Angebote und Leistungen für bestimmte Kunden so zu optimieren, dass Wettbewerber faktisch keine konkurrenzfähige Leistung anbieten können und damit vom Markt abgeschottet werden. Besonders bindungsgeneigt ist die Ausstattung der Kunden mit Software, die sich in ihrer Systematik hin zu Biotopen entwickelt und keine Alternativen mehr zulässt, zumindest keine Datenmigration ohne die Gefahr von Datenverlust oder Datendesorganisation. In vielen Fällen wird auch ein Systemwechsel allein an dem zu erwartenden wirtschaftlichen Aufwand scheitern. Wettbewerbsrechtlich kritisch sind insbesondere Vorgehensweisen zu beurteilen, bei denen der Anbieter verschiedene Programme und Funktionen miteinander so in Paketen verbindet, dass der Nutzer entweder keine Alternativen nutzen kann oder er darauf aus Bequemlichkeit verzichtet. Die Beispiele, in denen Anbieter von Software, Hardware, Netzleistungen und Speicherleistungen derartige Kopplungen lancieren, sind bereits heute im Markt von Verbrauchern, aber auch Unternehmen zahlreich. Wichtige Fragen sind zum Beispiel:

- Dürfen durch enge Verknüpfungen Mitbewerber faktisch ausgeschlossen werden?
- Wo ist die Grenze zum unzulässigen Verdrängungswettbewerb?
- Dürfen (und wenn ja, inwieweit) Erkenntnisse aus gelieferten Datenbeständen ausgewertet und (für andere Zwecke) verwertet werden?
- Wie können sich Datenzulieferer davor schützen, sich durch die Verfügbarmachung ihrer Daten / Programme selbst überflüssig zu machen?
- Wie sind Updates unter wettbewerbsrechtlichen Gesichtspunkten zu beurteilen?

Personal und Arbeit

Wenn Maschinen, Anlagen und Systeme immer weiter fortschreitend intelligente Funktionen übernehmen, werden sich neue Fragen zur menschlichen Arbeit ergeben. Bereits heute sind Menschen in den betrieblichen Prozesse intensiv maschinenbezogen tätig. Die Abläufe haben sich durch Informationstechnologie massiv verändert: einerseits sind zahlreiche einfache und höhere Tätigkeiten ersatzlos entfallen, andererseits sind für die heutigen Mitarbeiter die Anforderungen in der Handhabung von Systemen gestiegen. Dies gilt nicht nur in der Produktion, sondern auf allen Ebenen des Betriebes. Im Wegfall einfacher Arbeiten sehen Gewerkschaften und Sozialverbände Herausforderung für die Beschäftigungspolitik, in der steigenden Verdichtung der Kooperation von Mensch und Maschine eine ethische Herausforderung zur Erhaltung humaner Arbeitsplätze. Auf betrieblicher Ebene wird sich daher die schon heute bestehende Entwicklung und Diskussion fortsetzen: zu Steuerungen, Taktungen, Protokollierung, Sicherheitssysteme, Kommunikationserfassung und vieles mehr.
Dazu wichtige Fragen:

<u>Grundsatzfragen</u>

- Welche Rolle nimmt der Mensch im Werkprozess ein?
- Was passiert mit Arbeitsplätzen?

- Welche Ausbildungen / Studiengänge werden weniger / mehr nachgefragt werden?
- Besteht noch ein Bedarf für Betriebsräte?
- Wie verändern sich die Einflussmöglichkeiten von Betriebsräten / Gewerkschaften, wenn Arbeitskampf kein Druckmittel mehr ist?
- Welche Bedeutung haben Schwerpunktstreiks in einer (international) vernetzten Produktion?

Arbeitswelt

- Wie sollen / können / dürfen Arbeitsplätze ausgestaltet sein?
- Wie sollen / können / dürfen externe Plätze ausgestaltet sein?
- Wie kann / darf Überwachung zur Qualitätskontrolle ausgestaltet sein?
- Wie kann / darf Überwachung zum Arbeitsschutz ausgestaltet sein (Kameraüberwachung Mensch / Maschine)?
- Welche Informationsrechte / Mitwirkungsrechte / Mitbestimmungsrechte hat der Betriebsrat?
- Welche Fragen können / sollen von den Tarifpartner behandelt / festgelegt werden?
- Sollen die Vereinbarungen Allgemeingültigkeit haben?
- Erhalten Betriebsräte neue Kontrollrechte / Mitwirkungsrechte bei personenbezogenem Datenmanagement?

Steuern und Finanzen

Wenn in der vernetzten Wirtschaft Daten den wesentlichen Bestandteil einer technischen Funktionalität ausmachen oder als Wissen die Grundlage des Unternehmenserfolgs sind, stellt sich die Frage in neuer Dimension, wie der Wert solcher Datenbestände handelsrechtlich und steuerrechtlich zu beurteilen ist.

Steuern

Bereits heute können am Markt erworbene immaterielle Wirtschaftsgüter bilanziell aktiviert werden, für selbst geschaffene Wirtschaftsgüter hat das Unternehmen ein Wahlrecht zur Aktivierung oder Behandlung als Aufwand. Der Zuwachs oder aber die Irrelevanz von Datenbeständen sind dementsprechend zu behandeln. Für die steuerliche Anerkennung der bilanziellen Behandlung werden sich zahlreiche Grenzfälle mit Diskussionspotential ergeben. Fragen dazu sind

- Sind Datenbestände aktivierbare Vermögensgegenstände?
- Wann können / müssen sie abgeschrieben werden?
- Inwieweit beeinflussen Datenbestände / Datenströme aus internen / externen Quellen die Funktionalität und den Wert einer Maschine / Anlage / geistiger Rechte?

Finanzen

Welchen Wert Datenbestände für das Unternehmen und seine Geldgeber haben, muss im Einzelfall ermittelt werden. Datenbestände können eine entscheidende Grundlage für Kundennutzen, Markterfolg und Ertragskraft eines Unternehmens sein. Sie können aber auch für die reine Funktionalität von Maschinen, Anlagen und Systemen eine kritische Größe sein, wenn durch sie erst Maschinen produktiv eingesetzt werden können. Die Schwankungsbreiten zur Bewertung von Maschinen und Anlagen werden größer werden – das bedeutet eine herabgestufte Bewertung von Maschinen als Sicherheiten in der Kreditvergabe für Anlageninvestitionen. Daher dürfte die Finanzierung durch Bankkredite zurückgehen, während markt- und ertragsorientierte Finanzierungsmodelle weiter Platz greifen, insbesondere durch spezialisierte Leasinganbieter.

- Inwieweit beeinflussen Datenbestände / Datenströme aus internen / externen Quellen die Funktionalität und den Sicherungswert einer Maschine / Anlage / geistiger Rechte für Finanzierungszwecke?
- Inwieweit verändert dies das Anlagevermögen und das Eigenkapital?
- Müssen neue Finanzierungsinstrumente eingesetzt werden? Leasing, Factoring etc?
- Wie verändern sich Finanzierungsmodelle, wenn ein Betrieb virtuell organisiert ist: gemietete Räume, geleaste Maschinen, fremdgesteuerte Prozesse, ausgelagerte Daten und Prozesse (Cloud / Outsourcing), Einsatz von Subunternehmern und Zeitarbeitern?

Geschäftsführung und Aufsicht

Haftung der Geschäftsführung und Aufsichtsorgane

Grundsätzlich haben Vorstand und Geschäftsführer die Geschäfte der Gesellschaft und des Unternehmens mit der Sorgfalt eines ordentlichen Kaufmanns zu führen. Das bedeutet also, dass sie die Pflicht

haben, den Geschäftszweck bestmöglich zu verfolgen und dazu die richtigen und geeigneten Maßnahmen zu treffen. Fehler sind dabei nicht ausgeschlossen, wohl aber bei entsprechender Sorgfalt vermeidbare Fehler. Die Business Judgement Rule gesteht dem Geschäftsleiter also auch Irrtümer zu, allerdings keine beliebigen. Zur Vermeidung von Fehlern darf der Leiter auch nicht in Passivität verfallen, auch das Unterlassen kann einen Fehler darstellen, wenn Handeln geboten ist. Im Kontext von Industrie 4.0 bedeutet dies für Vorstände und Geschäftsführer eine ständige Herausforderung: einerseits dürfen sie das Unternehmen nicht von dynamischen Marktentwicklungen abkoppeln, andererseits müssen sie Wege und Methoden finden, mit oft noch unbekannten Risiken umzugehen. Fragen dazu sind:

- Welche Sorgfaltspflichten müssen Geschäftsführung und Vorstand bei Entscheidungen zur Einführung neuer Technologien beachten?
- Wo liegen die Grenzen der Business Judgement Rule?
- Welche Abwägungen muss ein Organ treffen?
- Welche Sicherungssysteme muss ein Organ einrichten?
- Wie muss es diese Systeme überwachen?
- Können sich Organe (GF / Vorstand) für Fehler / Schäden / Verletzungen aus fremdbestimmten Abläufen in ihrem Unternehmen freizeichnen?
- Welche Haftung trifft die Aufsichtsorgane?
- Wie sehen wirksame Haftungsübernahmen von Geschäftspartnern aus?
- Deckt die D&O Versicherung Haftungsfälle mit Fremdeinwirkung?

<u>Maßnahmen der Geschäftsführung / Legal Controlling</u>

Im Ergebnis müssen Vorstand und Geschäftsführer Methoden anwenden und Systeme einrichten, die ihnen eine möglichst weitreichende Einwirkungsmöglichkeit verschafft. Die Grundsätze des Risk Managements in der Skalierung von Schutzmaßnahmen gelten auch hier: technische Risiken vermeiden, rechtliche Risikokontrollen einrichten und Risikozuordnungen organisieren, wirtschaftliche Risiken finanziell absichern:

- Einrichtung von Sicherungs- und Kontrollsystemen als Risk-Management, Legal Controlling und Compliance Management
- Überwachung der Systeme als Risk-Management und Revision
- Sicherungs- und Kontrollvereinbarungen in Verträgen mit Geschäftspartnern
- Qualitäts- und Haftungsvereinbarungen in Verträgen mit Geschäftspartnern
- Monitoring von Vereinbarungen (Vertragscontrolling), Prozessen und Produkten
- Monitoring der rechtlichen Entwicklungen

Ausblick

Im Ergebnis wird das Recht eine flexible und belastbare Grundlage für die technologischen und wirtschaftlichen Entwicklungen unter Industrie 4.0 schaffen können. Vielfach werden sich bereits entwickelte und in der Praxis eingesetzte Methoden und Instrumente verwenden lassen, es wird aber auch bislang - zumindest in ihrer Dimension - weitgehend unbekannte Erscheinungen geben, für die das Rechte neue Instrumente schaffen muss. Dies wird in weitem Umfang durch vertragliche Rechtsgestaltung geschehen, teilweise wird der Gesetzgeber für Klarheit sorgen müssen. Vorstände und Geschäftsführer stehen in der Verantwortung, ihr Unternehmen wettbewerbsfähig und rechtssicher in die Zukunft zu führen.

+++

compact.
HERFURTH & PARTNER RECHT INTERNATIONAL.

caston.info

Beiträge zu Recht & Wirtschaft International finden Sie kostenfrei im Internet bei caston.info. Unsere Titelliste erhalten Sie auch per Mail.

IMPRESSUM

HERAUSGEBER

HERFURTH & PARTNER Rechtsanwaltsgesellschaft mbH
Luisenstr. 5, D-30159 Hannover
Fon 0511-30756-0 Fax 0511-30756-10
Mail info@herfurth.de, Web www.herfurth.de

Hannover · Göttingen · Brüssel
Member of the ALLIURIS GROUP, Brussels

REDAKTION

KORRESPONDENTEN

u.a. Amsterdam, Athen, Barcelona, Brüssel, Budapest, Bukarest, Helsinki, Istanbul, Kiew, Kopenhagen, Lissabon, London, Luxemburg, Lyon, Mailand, Madrid, Moskau, Oslo, Paris, Prag, Sofia, Stockholm, Warschau, Wien, Salzburg, Zug, New York, Toronto, Mexico City, Sao Paulo, Buenos Aires, Dubai, Kairo, New Delhi, Bangkok, Singapur, Peking, Shanghai, Tokio, Sydney, Johannesburg

VERLAG

CASTON GmbH, Law & Business Information
Luisenstr. 5, D-30159 Hannover,
Fon 0511 - 30756-50 Fax 0511 - 30756-60
Mail info@caston.info Web www.caston.info

compact.
HERFURTH & PARTNER RECHT INTERNATIONAL.

NEUERSCHEINUNG

Industrie 4.0 im Rechtsrahmen
Recht für die digitale Unternehmenspraxis

Industrie 4.0 ist für die meisten Unternehmen nicht mehr nur ein Schlagwort, sondern als Weg in die Digitalisierung von Produktion und Geschäftsprozessen bereits Realität.

Bei der Umsetzung der technologischen Entwicklungen entstehen allerdings zahlreiche neue rechtliche Fragen, die ein Unternehmen geklärt haben muss, um seine Ziele störungsfrei und sicher verfolgen zu können. Im Vordergrund steht die Sicherheit von Prozessen und Produkten - von größter Bedeutung ist aber auch der Umgang mit eigenen und fremden Daten und die Rechte daran. Je mehr sich ein Unternehmen digitalisiert, umso stärker verlagern sich seine Werte in diesem Bereich.

Der neue Report „Industrie 4.0 im Rechtsrahmen“ beschreibt in den verschiedenen Feldern, welche rechtlichen Rahmenbedingungen die Unternehmensprozesse steuern:

Besondere Herausforderungen entstehen aus dem Umgang mit autonomen Prozessen in der Leistungskette, im Qualitätsmanagement, in unternehmens- und in länderübergreifenden Beziehungen und Abläufen. Generierung, Besitz, Verwendung und Verwertung der großen Datenmengen werfen neue Fragen zu Schutz und Zugriffsrechten auf – und verlangen eine privatrechtliche vertragliche Gestaltung. Industrie 4.0 berührt aber auch wichtige andere Bereiche wie Personal und Arbeitsgestaltung, Wettbewerbsrecht, Finanzierung und Rechnungswesen und Beziehungen zu Providern, Plattformen und Netzen.
„Industrie 4.0 im Rechtsrahmen“ greift diese Fragen auf und gibt dazu aktuelle Lösungsansätze.

Industrie 4.0 im Rechtsrahmen
Leistungen, Daten, Strukturen

Herfurth, Ulrich (Hrsg)
Caston Edition, Hannover
ISBN 978-3-936647-03-7

Verlag:
Caston GmbH
Law & Business Information
D-30159 Hannover
Luisenstrasse 5
www.caston.info

compact.
HERFURTH & PARTNER RECHT INTERNATIONAL.

Inhalt

Querschnitt
- Rechtliche Aspekte zu Industrie 4.0

Betrieb & Systeme
- Verträge, Produktion, Lieferkette
- Netze, Telekom, Datensicherheit, Lizenzen

Technologie und Daten
- Datenschutz und Datensicherheit
- Dateneigentum
- Industrie 4.0 und das Immaterialgüterrecht
- Strafrechtsschutz für Computer und Daten

Finanzen
- Daten in Bilanz und Besteuerung

Markt und Wettbewerb
- Kartellrecht, Wettbewerbsrecht

Personal & Management
- Personal
- Geschäftsführung mit Legal Controlling

International
- Industrie 4.0 und Recht in den USA
- Industrie 4.0 und Recht in Brasilien
- Industrie 4.0 und Recht in China
- Industrie 4.0 und Recht in Russland
- Industrie 4.0 und Recht in Indien

Bestellung

Fax an 0511-307 56-10	*Stück*	*EUR/Stk*	*EUR /Ges*
▪ Industrie 4.0 in Eckpunkten, 2. Aufl. 2016-01		45,00	
▪ Industrie 4.0 im Rechtsrahmen, 1. Aufl. 2016-09		45,00	
Summe (inkl. Mwst u Versand im Inland)		XXXX	

Einige Beiträge finden sich in beiden Reports. Sie erhalten daher bei Bestellung **beider Publikationen** einen **Bonus** in Höhe von 20,00 EUR.

Name, Vorname*:

Position:

Firma*:

PLZ, Ort*:

Strasse*:

eMail*:

Unterschrift*:

*) Pflichtfelder

CASTON GmbH, Law & Business Information
Luisenstr. 5, 30159 Hannover
FON 0511 – 307 56-50 www.caston.info
FAX 0511 – 307 56-60 info@caston.info